JMH
F.# 2017R01764

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF

(1) ONE SAMSUNG DUOS MOBILE TELEPHONE, MODEL SM-J105H/DS, SERIAL NUMBER R21H30JCK3J, INCLUDING ANY SIM CARDS CONTAINED THEREIN;

(2) ONE ZTE MOBILE TELEPHONE, MODEL ZTE-N817, SERIAL NUMBER 320E67075138, INCLUDING ANY SIM CARDS CONTAINED THEREIN; AND

(3) ONE APPLE iPOD, MODEL NUMBER A1421, SERIAL NUMBER CCQKL01EF4K4,

SEIZED ON OR ABOUT OCTOBER 10, 2017, AND CURRENTLY IN THE CUSTODY OF THE FEDERAL BUREAU OF INVESTIGATION WITHIN THE EASTERN DISTRICT OF NEW YORK

17M989

APPLICATION FOR A SEARCH WARRANT FOR ELECTRONIC DEVICES

(Fed. R. Crim. P. 41; T. 18, U.S.C., § 875(b))

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, JACQUELINE ROSS, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—

electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("the FBI") and have been involved in the investigation of numerous cases involving the use of the Internet to commit violations of federal criminal laws, including but not limited to investigations involving the transmission of threats in interstate and foreign commerce via the Internet. I am familiar with the facts and circumstances set forth below from my participation in the investigation; my review of the investigative file, including the defendant's criminal history record; and from reports of other law enforcement officers involved in the investigation.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched is:

a. ONE SAMSUNG DUOS MOBILE TELEPHONE, MODEL SM-J105H/DS, SERIAL NUMBER R21H30JCK3J, INCLUDING ANY SIM CARDS CONTAINED THEREIN;

b. ONE ZTE MOBILE TELEPHONE, MODEL ZTE-N817, SERIAL NUMBER 320E67075138, INCLUDING ANY SIM CARDS CONTAINED THEREIN; AND

c. ONE APPLE iPOD, MODEL NUMBER A1421, SERIAL NUMBER CCQKL01EF4K4,

(hereafter, "the Devices") all seized on or about October 10, 2017, and currently in FBI custody within the Eastern District of New York. [1]

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. The FBI is investigating VICTOR CASILLAS for the transmission of extortionate threats in interstate commerce, in violation of 18 U.S.C. § 875(b).

7. On October 6, 2017, the FBI obtained an arrest warrant ("the Warrant") for CASILLAS based upon a criminal complaint sworn to by me before the Honorable Lois Bloom, United States Magistrate Judge for the Eastern District of New York, charging him with violating 18 U.S.C. § 875(b) ("the Complaint"). A copy of the Complaint is attached hereto as Exhibit 1. See ECF No. 1, No. 17-CR-605 (SLT) (Oct. 6, 2017).

8. As set forth in greater detail in the Complaint, there is probable cause to believe that CASILLAS has used one or more electronic devices to transmit extortionate threats to a corporation located in Colorado (referenced in the Complaint as "the Victim Company" and in

---

[1] On November 9, 2017, a draft copy of a substantially similar application was submitted to the Honorable Cheryl L. Pollak, United States Magistrate Judge for the Eastern District of New York ("the November 9 Draft"). The Devices were in FBI custody at an FBI facility in Manhattan, New York, on that date. Subsequent to the submission of the November 9 Draft, logistics rendered it impractical to bring the Devices to the Eastern District of New York to facilitate swearing out the proposed warrant on that same date, and the November 9 Draft was therefore withdrawn. To the best of the undersigned's knowledge, Magistrate Judge Pollak did not issue any ruling relating to the November 9 Draft.

the Indictment as "Victim Company #1").[2] See, e.g., Complaint, Ex.1, at ¶¶ 13-14 (referencing communications sent from Google email addresses to the Victim Company in which CASILLAS stated, on October 1, 2017, that Victim Company employees would be "LAYING IN THEIR CASKET ALL FOR A PETTY $100," and, on October 4, 2017, further threatening "GET READY FOR LAS VEGas part 2" and "MAYBE TODAY YOU WILL MEET YOU MAKER.").[3]

9. The facts set forth in the Complaint are incorporated herein in support of the requested warrant, and will only be restated as necessary.

10. Based on my participation in this investigation and information received from the Victim Company, I know that the threatening communications at issue in this investigation were sent via the Internet in and around and between September and October 2017. I also know that the substance of the communications relates to CASILLAS's use of a mobile application ("the Application"). The Application is accessible via the Internet and is promoted by the Victim Company. See Complaint, Ex. 1, at ¶¶ 3-4. I also know that CASILLAS originally registered his first account with the Victim Company, thereby making use of the Application, on or about September 19, 2014.

---

[2] The identity of the Victim Company is known to your affiant.

[3] I believe the reference to "Las Vegas" to be a reference to the mass shooting that occurred in Las Vegas, Nevada, on October 1, 2017.

11. On the evening of October 10, 2017, CASILLAS was arrested in Manhattan, New York, based upon the Warrant. CASILLAS was carrying the Devices when he was arrested, and the Devices were seized incident to his arrest.

12. Later that same evening, along with other agents and officers, I conducted an interview of CASILLAS at an FBI facility located in Manhattan, New York. CASILLAS was advised of his Miranda rights verbally and in writing. CASILLAS agreed to waive his Miranda rights, verbally and in writing, and agreed to speak with the investigating agents without the presence of his attorney.

13. In sum and substance and in part, CASILLAS admitted to sending threatening communications to the Victim Company. CASILLAS further admitted using one or more mobile telephones in connection with his use of the Application.

14. During the course of this interview, CASILLAS was shown printouts of some of the threatening communications at issue in this investigation, communications that had been received by the Victim Company via the Internet. In sum and substance and in part, CASILLAS admitted that he had written and sent these communications. CASILLAS further admitted that he had two mobile telephones, and that he had used one of them to send threatening communications to the Victim Company. CASILLAS further claimed that one of the mobile telephones was broken. CASILLAS denied using the Apple iPod that had been seized in connection with his arrest to send communications to the Victim Company, stating that it was "just for music."

15. CASILLAS was arraigned before the Honorable Peggy Kuo on October 11, 2017, and ordered detained. See ECF No. 5-9, No. 17-CR-605 (SLT).

16. On November 2, 2017, a grand jury sitting in the Eastern District of New York returned an indictment charging CASILLAS with the same offense ("the Indictment"). A copy of the Indictment is attached hereto as Exhibit 2. See ECF No. 10, No. 17-CR-605 (SLT) (Nov. 2, 2017).

17. Based on the facts set forth above, there is probable cause to believe that the Devices described in Attachment A contain evidence of CASILLAS's use of the Application, including but not limited to evidence of access to the Application and to the email accounts used to send the threatening communications to the Victim Company that are at issue in this investigation, as more fully described in Attachment B.

18. Based on my training and experience, as well as my review of open source information, I know that the Devices have capabilities that allow them to access the Internet.

19. The Devices are currently in the lawful possession of the FBI, having come into FBI custody incident to CASILLAS's arrest as described above. Therefore, while the FBI might already have all necessary authority to examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

20. The Devices are currently in FBI custody within the Eastern District of New York. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the FBI.

TECHNICAL TERMS

21. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by

connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that

are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP

addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

22. Based on my training, experience, and research, and from consulting with other agents familiar with Samsung and ZTE brand mobile telephone devices, I know that the SAMSUNG DUOS MOBILE TELEPHONE, MODEL SM-J105H/DS, SERIAL NUMBER R21H30JCK3J and ZTE MOBILE TELEPHONE, MODEL ZTE-N817, SERIAL NUMBER 320E67075138, both seized incident to CASILLAS's arrest, both have capabilities that allow each device to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA.

23. Based on my training, experience, and research, and from consulting the manufacturer's specifications which are available online at https://www.apple.com/ipod-touch/specs/, I know that the APPLE iPOD, MODEL NUMBER A1421, SERIAL NUMBER CCQKL01EF4K4 seized incident to CASILLAS's arrest has capabilities that allow it to serve as a digital camera, portable media player, GPS navigation device, and PDA.

24. In my training and experience, examining data stored on devices of these types can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

25. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to send extortionate communications via the Internet in violation of 18 U.S.C. § 875(b), the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

28. *Manner of execution.* Because this warrant seeks only permission to examine Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

REQUEST FOR LIMITED SEALING

29. Because Attachment B to the requested warrant identifies the Victim Company by name, if and when the Court approves the requested warrant, I respectfully request permission to file the unredacted copy of Attachment B under seal. I further request permission to substitute a redacted copy of the warrant on the public docket of this matter, wherein the name of the Victim Company will be redacted from the text of Attachment B where it appears. A copy of the proposed public copy of Attachment B, as redacted, is included herein as Exhibit 3.

CONCLUSION

30. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

JACQUELINE ROSS
Special Agent
FBI

Subscribed and sworn to before me
on November 20, 2017:

THE HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is:

a. ONE SAMSUNG DUOS MOBILE TELEPHONE, MODEL SM-J105H/DS, SERIAL NUMBER R21H30JCK3J, INCLUDING ANY SIM CARDS CONTAINED THEREIN;

b. ONE ZTE MOBILE TELEPHONE, MODEL ZTE-N817, SERIAL NUMBER 320E67075138, INCLUDING ANY SIM CARDS CONTAINED THEREIN; AND

c. ONE APPLE iPOD, MODEL NUMBER A1421, SERIAL NUMBER CCQKL01EF4K4,

(hereafter, "the Devices") all seized on or about October 10, 2017, and currently in FBI custody within the Eastern District of New York.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

See
Exhibit 3
Attachment B

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

EXHIBIT 1

SDD:JMH
F. #2017R01764

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA

- against -

VICTOR CASILLAS,

Defendant.

----------X

TO BE FILED UNDER SEAL

COMPLAINT

(18 U.S.C. § 875(b))

No. 17 M 988

EASTERN DISTRICT OF NEW YORK, SS:

JACQUELINE ROSS, being duly sworn, deposes and states that she is a Special Agent with the Federal Bureau of Investigation, duly appointed according to law and acting as such.

On or about and between September 26, 2017, and October 4, 2017, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VICTOR CASILLAS, knowingly and with intent to extort money from a corporation located in Colorado ("the Victim Company"), did transmit in interstate and foreign commerce, via the Internet, one or more communications containing threats to injure one or more employees of the Victim Company.

(Title 18, United States Code, Section 875(b))

The source of your deponent's information and the grounds for her belief are as follows:[1]

1. I am a Special Agent with the Federal Bureau of Investigation ("the FBI") and have been involved in the investigation of numerous cases involving the use of the Internet to commit violations of federal criminal laws, including but not limited to investigations involving the transmission of threats in interstate and foreign commerce via the Internet. I am familiar with the facts and circumstances set forth below from my participation in the investigation; my review of the investigative file, including the defendant's criminal history record; and from reports of other law enforcement officers involved in the investigation.

2. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 875(b), the transmission of extortionate threats in interstate commerce, have been committed, are being committed, and will be committed by VICTOR CASILLAS. Specifically, CASILLAS is believed to have sent threatening communications via the Internet to one or more employees of the Victim Company. The threats, in sum and substance, state that CASILLAS will murder one or more employees of the Victim Company if his demands for money from the Victim Company are not met, as more fully set forth below.

3. Based on information provided by the Victim Company and open source information associated with the Victim Company's website, I know that the Victim

---

[1] Because the purpose of this Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

Company markets a mobile application, accessible via the Internet, that allows users to review and obtain promotional sales offers from various retailers. Users may also earn credits from the Victim Company by submitting proofs of purchases made using such offers to the Victim Company. Over time, users may exchange those credits for money.

4. Based on information provided by the Victim Company, I also know that the Victim Company gives users credits, exchangeable for money, for referring other users to make use of the Victim Company's services. The Victim Company refers to these as "referral bonuses."

5. Based on information provided by the Victim Company, I know that the Victim Company has received a number of threatening communications from an individual using the name "Victor Casillas." Specifically, records from the Victim Company reflect that a user named "Victor Casillas" opened his first account on or about September 19, 2014, using the email address viconefans187@gmail.com ("Casillas Account A"). Victim Company records also reflect that a user named "Victor Casillas" subsequently opened approximately fourteen additional accounts using various email addresses in 2016 and 2017.

6. In late 2016 and early 2017, the Victim Company undertook a review of several of the "Victor Casillas" accounts, and concluded that they represented a potentially fraudulent effort to generate referral bonuses. The user of the account, whom I believe to be CASILLAS, communicated via Casillas Account A in connection with the disputed bonuses. During the course of the dispute, the user circulated a draft letter to a third party company, one of the retailers from whom users of the Victim Company's services can obtain offers. In sum and substance, the letter states CASILLAS's complaints about the Victim Company.

In the course of the letter, CASILLAS identified various social media accounts as belonging to him, including but not limited to a Facebook Account with the vanity username "vicone954" ("the Casillas Facebook Account"), and a personal website ("the Casillas Website").

7. Based on information provided by the Victim Company, I know that the Victim Company collected publicly-available photographs from the Casillas Facebook Account during the course of the dispute. Those photographs, which depict an individual I believe to be VICTOR CASILLAS, were provided to me by the Victim Company and are reproduced below:

8. In early 2017, the Victim Company attempted to resolve the dispute by issuing a $40 payment and closing the related user accounts. In connection with the payment, the Victim Company required the user, whom I believe to be CASILLAS, to provide a telephone number to facilitate transfer of the payment via an Internet payment application, Paypal. CASILLAS provided the telephone number (347) 564-1718 ("the 1718 Number") to the Victim Company.

9. Over the course of 2017, additional accounts were created at the Victim Company by an individual using the user name "Victor Casillas." One of these accounts was associated with the email address skrillavic187@gmail.com ("Casillas Account B").[2] The Victim Company, after a review of the accounts, again concluded that they represented a potentially fraudulent attempt to generate referral bonuses. They therefore locked the user accounts, including the one associated with Casillas Account B. On or about September 26, 2017, the Victim Company advised the user of Casillas Account B that it was deactivating the associated account.

10. Over the course of the next several days, the user of the closed accounts, whom I believe to be CASILLAS, caused the following threatening communications, among others, to be sent to the Victim Company by means of the Internet, either via the email address associated with Casillas Account B, or via the Victim Company's mobile or web-based application:

---

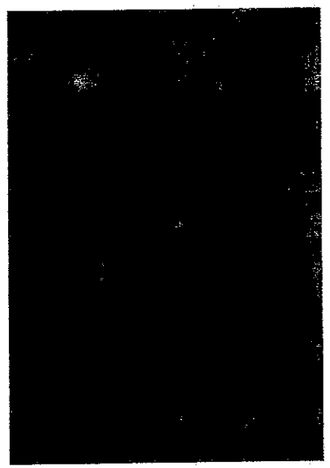
[2] Based on my training and experience, I know that the numeric sequence "187" can sometimes be used as shorthand for a murder or other unlawful death, based on the numeration of the crime of murder in the California Penal Code, see Cal. Penal Code § 187, and its usage in common American slang.

Date	Content[3]
Sept. 26, 2017	such a cowardly act on your behalf whats your name btw? I wanna know who your spouse and children are too and I'm not asking you I'm telling you, I want to know who your parents are as well if the pieces of trash are even still alive (for now) for that matter,
Sept. 27, 2017	IVE ARRIVED IN DENVER STOLEN FUNDS WILL BE GIVEN TO THE EARNER I HOPE YOU CLEARLY UNDERSTAND IF THE LAW DONT GET YOU.....I WILL!!!!....THE ACT THAT WAS COMMITED WAS COLD HEARTED SADISTIC, FALSE, I DID NO SUCH THING OF DUPLICATING [Victim Company] ACCOUNTS..... YOU WILL GIVE MY GODAM FUNDS YOU SONS OF BITCHES, I SPENT 100'S OF DOLLARS AND EVEN TOOK ME 3 HOURS TO SHOP ON [Third-Party Website] THROUGH YOUR MOBILE APP..... YOU AINT HEARING ME?? YOU DONT FEEL MY PAIN?..... SO BE IT....SEE YOU ALL SOON. [The communication was accompanied by the photograph of the two submachine guns depicted below][4] 
Sept. 27, 2017	THIS IS NOT A JOKE NO 48 HOURS TOOK ME 3 HOURS TO ORDER FROM [Third Party Website], YO9U GUYA ARE NOT GETTING AWAY WITH THIS, I WILL BE PURCHASING MY AIRLINE TICKETS WITHIN THE NEXT HALF]HOUR

---

3 The content of the messages quoted herein is replicated herein as in the original, including typographical errors, except where indicated.

4 Further investigation revealed that this photograph of what appear to be two MAC-11 submachine guns may be obtained from open-source images accessible via the Internet.

Date	Content[3]
Sept. 27, 2017	KEEP UP THE STALL, ITLL BE THE LAST TIME YOU EVER DO.... [The communication was accompanied by the photograph of a submachine gun, with silencer, and two high-capacity magazines, depicted below][5] 
Sept. 28, 2017	I AM HERE IN COLORADO..... I AM READY EQUPPIED AND READY TO STRIKE (RETALIATE TO RECOVER STOLEN FUNDS OF 113 BY CRIMINALS OF [Victim Company] INC) IN ANY GIVING MOMENT.....YOU HAVE TIL THE END OF THIS MONTH TODO THE RIGHT THING....again i repeat the Gods honest RIGHT THING..... HOPE YOU VALUE THE LIVES OF YOUR (CROOKED) EMPLOYEES.,

11. On September 28, 2017, at approximately 1:35 p.m., the Victim Company received a communication via the Internet stating: "TOP TARGETS FOR SNIPER . . . NAMES OF FIRST ROW OF SERIAL DEATHS BY ASSASIATION," going on to list

---

5 Further investigation revealed that this photograph of what appears to be a MAC-10 submachine gun may be obtained from open-source images accessible via the Internet.

three names of Victim Company employees, followed by the warning "PLEASE TELL LOVED ONES TO START PICKING OUT A NICE BEAUTIFUL CASKET AND PLAN A DECENT FUNERAL."

12. The message continued with four additional names of Victim Company employees, including photographs. One of the employee names was suffixed with the word "Decapitation."

13. On October 1, 2017, the Victim Company received a communication from skrillavic187part2killibottas@gmail.com ("Casillas Account C"), which stated, among other statements: "I JUST CANT WAIT TO REALITY HITS AND YOU (THE CURRENT READER) OR CO WORKERS ARE LAYING IN THEIR CASKET ALL FOR A PETTY $100 . . . HOPE IT IS WORTH IT . . .P.S. SEE YOU GUYS SOON!"

14. On October 4, 2017, the Victim Company received a communication from the email address associated with Casillas Account B, titled "GET READY FOR A LAS VEGAS REPEAT (Final Warning)," stating "I I STILL HAVE NOT RECIEVED MY GOD DAM FUNDS.....ASSHOLES . . . WELL GET READY 4 LAS VEGas part 2 ....MAYBE TODAY YOU WILL MEET YOU MAKER."[6] The Victim Company received IP Address information associated with this message, which indicated that the message originated in Brooklyn, New York.

15. The messages summarized above reflect a representative sample of the communications received by the Victim Company relating to the closed "Victor Casillas" accounts. Based on information provided by the Victim Company, I know that several

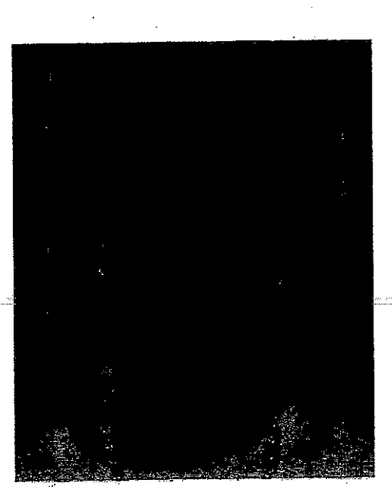
---

[6] I believe the reference to "Las Vegas" to be a reference to the mass shooting that occurred in Las Vegas, Nevada, on October 1, 2017.

additional messages, similar in form and content, were received relating to the closed "Victor Casillas" accounts.

16. The Victim Company recorded IP Address and GPS location information associated with each of the "Victor Casillas" accounts at the Victim Company. Based on my review of that GPS location information, each was created from an IP address located within the boroughs of Manhattan, Brooklyn, or Staten Island.

17. From information provided by New York State authorities, I know that VICTOR CASILLAS has been issued a New York State non-driver identification card listing a registered address on Monument Walk in Brooklyn, New York, and bearing the photograph depicted below:



18. Based on my review of the above photograph, I believe the person depicted is the same individual depicted in the photographs collected from the Casillas Facebook Account referenced in paragraph 7, above, that is, VICTOR CASILLAS. Moreover, on October 5, 2017, I accessed publicly-available information and photographs

associated with the Casillas Facebook Account. In sum and substance, several photographs depicted CASILLAS. Among other photographs, one of the photographs depicted in paragraph 10, above, was displayed. The Casillas Facebook Account also identified a number of other social media accounts with various services, frequently under the username or handle of "vicone187". The Casillas Facebook Account also lists the information for the Casillas Website referenced in paragraph 6, above.

19. On October 5, 2017, I obtained information from the service provider for the 1718 Number provided by CASILLAS to the Victim Company, pursuant to 18 U.S.C. § 2702. The information revealed that the 1718 Number is still active, and that it is registered to "Victor Casillas" with the same address identified on the New York State identification described in paragraph 17, above.

WHEREFORE, your deponent respectfully requests that the defendant VICTOR CASILLAS, be dealt with according to law.

JACQUELINE ROSS
Special Agent
Federal Bureau of Investigation

Sworn to before me this
6th day of October, 2017

THE HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

EXHIBIT 2

AAS:JMH
F. #2017R01764

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA

- against -

VICTOR CASILLAS,

Defendant.

----------X

INDICTMENT
Cr. No. CR 17 605
(T. 18, U.S.C., §§ 875(b) and 3551 et seq.)

TOWNES, J

POLLAK, M.J.

U.S. DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
2017 NOV -2 AM 11:5
FILED
CLERK

THE GRAND JURY CHARGES:

TRANSMISSION OF EXTORTIONATE THREATS
IN INTERSTATE COMMERCE

In or about and between September 2017 and October 2017, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VICTOR CASILLAS did knowingly and intentionally transmit in interstate and foreign commerce, with the intent to extort money and other things of value from a person, firm, association or corporation, to wit: Victim Company #1, a corporation the identity of which is known to the Grand Jury, one or more electronic communications containing one or

more threats to injure the person of another, to wit: threats to injure one or more employees of Victim Company #1.

(Title 18, United States Code, Sections 875(b) and 3551 et seq.)

A TRUE BILL

FOREPERSON

BRIDGET M. ROHDE
ACTING UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK

F. # 2017R01764
FORM DBD-34
JUN. 85

No.

UNITED STATES DISTRICT COURT

EASTERN *District of* NEW YORK

CRIMINAL DIVISION

THE UNITED STATES OF AMERICA

vs.

VICTOR CASILLAS,

Defendant.

INDICTMENT

(T. 18, U.S.C., §§ 875(b) and 3551 et seq.)

A true bill.

_____ *Foreperson*

Filed in open court this _____ *day,*

of _____ *A.D. 20* _____

_____ *Clerk*

Bail, $ _____

_____

J. Matthew Haggans, Assistant U.S. Attorney (718) 254-6127

3

EXHIBIT 3

ATTACHMENT B

1. All records on the Device(s) described in Attachment A that relate to violations of 18 U.S.C. § 875(b) and involve VICTOR CASILLAS since September 19, 2014, including:

a. All records of access to any mobile application or Internet website associated with [redacted] (hereafter "the Victim Company");

b. All records of any electronic communications sent to or received from the Victim Company, including emails, text messages, SMS messages, iMessages, or other text-based communications;

c. All records of any attachments to any electronic communications referenced in 1(a) and 1(b) above, including but not limited to photographs of firearms or other weapons; and

JR

d. Any information recording VICTOR CASILLAS's whereabouts, his travel schedule, and his residence in and around and between December 2016 and October 2017.

2. Evidence of user attribution showing who used or owned the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Internet to communicate with Google, Yahoo!, AOL and Hotmail email servers and/or Victim Company servers, including:

a. records of Internet Protocol addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.